Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

24 FEB 1984

CONFIDENTIAL

NATIONAL POLICY ON TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS SECURITY (U)

Recent advances in microelectronics technology have stimulated an unprecedented growth in the demand for telecommunications and information processing services within the Government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information proccessing systems are highly susceptible to interception, electronic penetration, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. [redacted] 25X1

These systems process and communicate classified National security information, other sensitive information concerning vital interests of the United States, and the private information of US persons and businesses. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially by hostile intelligence services, does serious damage to the United States and its interests. A comprehensive and coordinated approach must be taken to protect the Nation's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities. [redacted] 25X1

NSC review

25X1

WARNING NOTICE
INTELLIGENCE SOURCES
OR METHODS INVOLVED

CONFIDENTIAL

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

This Directive provides initial objectives and policies to guide the conduct of National activities directed toward safeguarding systems which process or communicate sensitive information, establishes a mechanism for policy development and assigns responsibilities for implementation. [redacted] 25X1

1. Objectives. Security is a vital element of the operational effectiveness of the National security activities of the Government and of military combat readiness. Assuring the security of telecommunications and automated information systems which process and communicate classified National security information, other sensitive Government information, and certain private information of US persons is a key national responsibility. I, therefore, direct that the Nation's capabilities for securing telecommunications and automated information systems against technical exploitation threats be maintained and improved as necessary to provide for:

a. A reliable and continuing capability to assess threats and vulnerabilities, and to implement appropriate, effective countermeasures.

b. A superior technical base within the Government to achieve this security, and a superior technical base within the private sector in areas which complement and enhance Government capabilities.

c. A more effective application of Government and private resources.

d. Support and enhancement of other policy objectives for national telecommunications and automated information systems. (U)

2. Policies. In support of these objectives, the following policies are established:

a. Systems which generate, store, process, transfer or communicate classified information in electrical form shall be secure or protected by such means as are necessary to prevent compromise and exploitation.

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

b. Systems handling other Government-derived information, the loss of which could adversely affect the national interest or the rights of US persons, shall be protected against the threat of exploitation and the associated potential damage.

c. The Government shall take necessary steps to identify systems which handle non-Government information, the loss of which could adversely affect the National interest or the rights of US persons, and formulate strategies and measures for providing protection against the threat of exploitation and the associated potential damage. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-Governmental systems would be in the national interest, the private sector shall be encouraged and assisted in undertaking the application of such measures. 25X1

3. Implementation. This Directive establishes a senior level steering group; an interagency group at the operating level; and an executive agent. 25X1

4. Systems Security Steering Group.

a. A Systems Security Steering Group consisting of the Secretary of State, the Secretary of Defense, the Secretary of the Treasury, the Director of the Office of Management and Budget, the Director of Central Intelligence, and chaired by the Assistant to the President for National Security Affairs is established. The Steering Group shall:

(1) Oversee and ensure the implementation of this Directive.

(2) Monitor the activities of the operating level National Telecommunications and Information Systems Security Committee (NTISSC) and provide guidance for its activities in accordance with the objectives and policies contained in this Directive.

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

(3) Review and evaluate the security status of National telecommunications and automated information systems with respect to established objectives and priorities, and report findings and recommendations through the National Security Council to the President.

(4) Review and approve consolidated resources program proposals, and other matters referred to it by the NTISSC.

(5) On matters pertaining to the protection of intelligence sources and methods be guided by the policies of the Director of Central Intelligence.

(6) Interact with the Steering Group on National Security Telecommunications to ensure that the objectives and policies of this Directive and NSDD-97, National Security Telecommunications Policy, are addressed in a coordinated manner.

(7) Recommend for Presidential approval additions or revisions to this Directive as National interests may require. [redacted] 25X1

b. A representative of the Executive Agent for Telecommunications and Information Systems Security shall function as the secretary to the Steering Group. [redacted] 25X1

5. The National Telecommunications and Information Systems Security Committee.

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be chaired by a representative of the Secretary of Defense and shall be comprised of a voting representative of each of the following:

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

The Secretary of State
The Secretary of the Treasury
The Attorney General
The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy
The Director of Central Intelligence
Chairman, Joint Chiefs of Staff
Administrator, General Services Administration
Director, Federal Emergency Management Agency
The Chief of Staff, United States Army
The Chief of Naval Operations
The Chief of Staff, United States Air Force
The Chief of Staff, United States Marine Corps
Director, National Security Agency
Manager, National Communications System

25X1

b. The Committee shall:

(1) Develop such specific operating policies, objectives, and priorities as may be required to implement this Directive.

(2) Submit annually to the Steering Group an evaluation of the status of National telecommunications and automated information systems security with respect to established objectives and priorities.

(3) Approve the release of sensitive systems security information, techniques and materials to foreign governments or international organizations (except in intelligence activities sponsored by the Director of Central Intelligence).

(4) Establish and maintain a national system for promulgating the operating policies, directives, and guidance which may be issued pursuant to this Directive.

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

(5) Establish two permanent, major subcommittees that will interact closely with one another to ensure recommendations concerning implementation of protective measures are combined and are coordinated in both areas where appropriate and shall consider any differences in the level of maturity of the technologies to support such implementations. One subcommittee will focus on telecommunications security while the other subcommittee will focus on information processing security. NTISSC nominations to chair these two subcommittees are subject to Steering Group confirmation. The Committee may establish other permanent and temporary subcommittees, as necessary to discharge its responsibilities, without Steering Group confirmation.

(6) Make recommendations to the Steering Group on Committee membership and establish criteria and procedures for permanent observers, from other Departments or Agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman.

c. The NTISSC shall develop and submit to the Steering Group a proposed National telecommunications security program for each fiscal year, that includes: 25X1

(1) The quantity and types of equipment required as determined by the Heads of Departments and Agencies.

(2) An estimate of the total funds required to support the program.

(3) An estimate of the funding that will be provided by Departments and Agencies.

(4) An estimate of deficits in proposed funding and a proposal for providing supplemental funding to cover any deficits from other programs, or seek relief from OMB.

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

(5) Ongoing funding of the Communications Security Utility-Program (CUP) that is adequate to ensure that:

a) All telecommunications security equipment is procured in the most cost effective manner.

b) There is sufficient procurement of all telecommunications security equipment over the life of the equipment to maintain a viable industrial support base.

c) Provisions for ensuring the changes in requirements of one Department or Agency do not adversely effect the total procurement cycle or the programs/budgets of another Department or Agency.

e. The Committee shall have a permanent secretariat composed of personnel from the Departments and Agencies represented on the Committee. (U)

6. The Executive Agent of the Government for Telecommunications and Information Systems Security. The Secretary of Defense is the Executive Agent of the Government for Communications Security under authority of Executive Order 12333. By authority of this Directive he shall serve an expanded role as Executive Agent of the Government for Telecommunications and Information Systems Security. In this capacity he shall act in accordance with policies and procedures established by the Steering Group and the NTISSC to:

a. Develop minimum telecommunications and automated information system security standards and doctrine for NTISSC review and approval.

b. Undertake research and development of security techniques and equipment as directed by the Steering Group and the NTISSC.

c. Assist in the efforts of Government technical centers related to telecommunications and automated information systems security.

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

d. Upon the request of the Head of a Department or Agency, examine that Department's or Agency's Government telecommunications and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with the law and other applicable Directives.

e. Act as the Government focal point for all matters related to telecommunications and automated information systems security.

f. Operate a central technical center to evaluate the security of telecommunications and automated information systems.

g. Enter into agreements for the procurement of technical security material and equipment to meet the identified requirements of other Departments and Agencies. [redacted] 25X1

7. The Heads of Federal Departments and Agencies Shall:

a. Be responsible for achieving and maintaining an acceptable security posture for telecommunications and automated information systems within their Departments or Agencies.

b. Ensure that the policies, standards and doctrines issued pursuant to this Directive are implemented within their Departments or Agencies.

c. Provide to the Intelligence Community Threat Assessment Center (ICTAC), such information as it may require to discharge responsibilities assigned herein. [redacted] 25X1

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

8. Additional Responsibilities.

a. The Intelligence Community shall operate a central threat assessment center to assess and disseminate information on hostile threats to National telecommunications and information systems security. The ICTAC shall solicit from the Heads of Departments and Agencies such information and technical support as may be needed to discharge the responsibilities assigned herein.

b. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue for public use standards for the security of telecommunications and other automated information systems, as approved by the NTISSC.

c. The Director, Office of Management and Budget shall review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein. [redacted] 25X1

9. Nothing in this Directive:

a. Alters the existing authorities of the Director of Central Intelligence.

b. Provides any Party mentioned in this Directive the authority to inspect the personnel, systems, equipment or facilities of other Departments and Agencies without approval of the head of such Department or Agency, or the authority to request or collect information concerning their operations.

c. Amends or contravenes the provisions of existing directives which may pertain to the financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

d. Is intended to establish additional review processes for the procurement of automated information processing systems. [redacted] 25X1

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

10. For the purpose of this Directive, the following terms shall have the meanings indicated:

a. Telecommunications means the transmission, communication, or processing of information, including the preparation of such information therefore, by electrical, electromagnetic, electromechanical or electro-optical means.

b. Automated Information Systems means systems which create, prepare, or manipulate information for purposes other than telecommunications, and includes computers, word processing systems, other information handling systems, and associated equipment.

c. Telecommunications and Automated Information Systems Security means protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and information.

d. Technical Security Material means equipment components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and automated information processing systems. (U)

e. Government means the Executive Branch of the Government of the United States of America.

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

12. The Interagency Committee on Foreign Real Estate Acquisitions in the United States [redacted] 25X1
[redacted] shall be reconstituted to serve as an 25X1
interagency policy coordination committee under the chairmanship of the Department of State, with representation from the Department of Defense, the Department of Justice/Federal Bureau of Investigation, the Director of Central Intelligence, the National Security Agency, and the Assistant to the President for National Security Affairs. It shall provide policy guidance for implementation by the Office of Foreign Missions of the Department of State or other appropriate organizations on proposals for foreign real estate acquisitions, by lease or purchase, which present a security threat to US telecommunications and automated information systems or are of counterintelligence interest. [redacted] 25X1

13. The functions of the National Communications Security Committee (NCSC) are subsumed by the NTISSC. The policies established under the authority of the NCSC shall remain in effect until rescinded or modified by the NTISSC. (U)

14. Except for protection activities mandated by and begun
25X1 under [redacted] that Directive is hereby superseded. (U)

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8

STAT

STAT

25X1

ROUTING AND TRANSMITTAL SLIP Date 2/24/84

TO: (Name, office symbol, room number,	Initials	Date
1.		2/1
2. C/IPPG		
3.		
4.		
5.		

Action	File	Note and Return
Approval	For Clearance	Per Conversation
As Requested	For Correction	Prepare Reply
Circulate	For Your Information	See Me
Comment	Investigate	Signature
Coordination	Justify	

REMARKS

Herewith, the latest on [redacted] COMSEC is getting its comments together to meet the 27 February 84 deadline.

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
[redacted]	Phone No.

5041-102

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

☆ GPO : 1983 O - 381-529 (301)

Approved For Release 2007/07/25 : CIA-RDP87B01034R000700080021-8